Unconditionally secure single qubit quantum secret sharing

Guang Ping He*
School of Physics & Engineering and Advanced Research Center, Sun Yat-sen University, Guangzhou 510275, China

Z. D. Wang†
Department of Physics and Center of Theoretical and Computational Physics, The University of Hong Kong, Pokfulam Road, Hong Kong, China

Analyzing carefully an experimentally feasible non-entangled single qubit quantum secret sharing protocol and its modified version [Phys. Rev. Lett. **95**, 230505 (2005); *ibid.* **98**, 028902 (2007)], it is found that both versions are insecure against coherent attacks though the original idea is so remarkable. To overcome this fatal flaw, here we propose a secure protocol with a distinct security checking strategy, which still involves single qubit operations only, making it possible to achieve unconditionally secure quantum secret sharing with current technology.

PACS numbers: 03.67.Hk,03.67.Dd

Consider a committee of N members, one of which has a set of secret data, e.g., the password for a locker or the access code for a computer program. He wants others to share the data in such a way that the data can be regained if all of these $N-1$ members collaborate, while any subset of less than $N-1$ members cannot do so successfully. This is a typical secret sharing problem. Secret sharing is also an element for building up many other complicated cryptographic protocols. But in classical cryptography, unconditional security cannot be achieved in principle. With the fascinating development of quantum cryptography, using quantum methods to achieve secure secret sharing has caught great interests both theoretically and experimentally[1, 2, 3, 4, 5, 6]. However, most of the quantum secret sharing (QSS) protocols have to rely on entangled quantum states. So far, the preparation of entangled states has still been quite inconvenient in practice, and it has been even harder to store them for more than a brief time, especially when different parts of the entangled states are shared and kept separated by different participants. For this reason, even though some of these protocols can be demonstrated in laboratory, they are likely still far from practical applications.

Recently, a novel QSS protocol was proposed and experimentally demonstrated by Schmid *et al.*[7], which involves non-entangled single qubits only. Thus the protocol is very promising in practice. However, a subtle security loophole was found later[8]. A modification on the original protocol was then proposed by Schmid *et al.*[9]. But here it will be shown that the modified one is even less secure than the original one. Most important, we propose a new protocol with a distinct security checking strategy, which closes the security loophole successfully and makes the protocol unconditionally secure. Meanwhile, the great feasibility of the original protocol is still maintained. Therefore, the present protocol is of significance both theoretically and practically.

Let us first recall briefly the original QSS protocol proposed by Schmid *et al.*[7]. The goal of the proposal is that: after each of N participants inputs the secret data, any $N-1$ participants should be able to infer the secret input of the remaining participant if and *only if* they collaborate. Let $|0\rangle$ and $|1\rangle$ denote the two orthonormal states of a qubit. Define $|\pm x\rangle = (|0\rangle \pm |1\rangle)\sqrt{2}$ and $|\pm y\rangle = (|0\rangle \pm i\,|1\rangle)/\sqrt{2}$. *The original protocol* is actually stated as follows.

(1) The first participant R_1 prepares a single qubit in the state $|+x\rangle$.

(2) The qubit is passed through the N participants sequently. Each participant R_j $(j = 1, ..., N)$ chooses the secret data $\varphi_j \in \{0, \pi/2, \pi, 3\pi/2\}$, and acts on the qubit with the unitary phase operator

$$\hat{U}_j(\varphi_j) = \begin{cases} |0\rangle \to |0\rangle \\ |1\rangle \to e^{i\varphi_j}\,|1\rangle \end{cases} . \qquad (1)$$

(3) The last participant R_N measures the qubit in the basis $|\pm x\rangle$. This completes one run of the qubit communication.

(4) Each participant divides his action for every run into two classes: a class X corresponding to $\varphi_j \in \{0, \pi\}$ and a class Y corresponding to $\varphi_j \in \{\pi/2, 3\pi/2\}$. They broadcast the class of their action for each run in random order, but keep the particular value of φ_j secret.

(5) With the announced classification, they determine which runs are valid runs that satisfy the condition $\left|\cos(\sum_j^N \varphi_j)\right| = 1$ and lead to a deterministic measurement result of R_N.

(6) The security check: the participants choose a subset of valid runs, and announced the value of φ_j of each participant in random order. They make comparison between these values and the measurement result in step (3) to detect cheating.

*Electronic address: hegp@mail.sysu.edu.cn
†Electronic address: zwang@hkucc.hku.hk

(7) The task of secret sharing is achieved with the remaining valid runs. When any subset of $N-1$ participants wants to infer the choice of φ_R of the remaining participant, they reveal among themselves their values of φ_j. In the case in which this subset contains the last participant, he reveals the measurement result in step (3).

A significant merit of this protocol lies in that only the local manipulation of phases on a communicated single qubit is needed, and thus it is very feasible for practical realization. Unfortunately, although the protocol can indeed accomplish the task that any $N-1$ participants are able to infer the choice of φ_R of the remaining participant if they collaborate, it was shown in Ref.[8] that a subset of less than $N-1$ participants may also reach this goal in certain cases, namely, the protocol does not reach the security it was supposed to have. The cheating strategy in Ref.[8] is outlined below.

Cheating strategy A:

Suppose that the kth participant R_k ($k \in \{2, ..., N-1\}$) is dishonest. According to Eq. (1), the state of the qubit he receives from R_{k-1} in step (2) is $|\chi_{k-1}\rangle = (|0\rangle + e^{i(\sum_j^{k-1}\varphi_j)}|1\rangle)/\sqrt{2}$. In contrast to what he should do in the honest protocol, he does not apply the operator $\hat{U}_k(\varphi_k)$ on it to obtain χ_k and then pass it to the next participant R_{k+1}. Instead, he keeps the qubit unmeasured. He also prepares an EPR pair $|\psi\phi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, and sends the second qubit ϕ to R_{k+1} as χ_k while keeping ψ to himself. In step (4) when it is time for him to broadcast the class of his action, since the order in which the participants announce the classification is randomly chosen, there can be two cases:

(i) Some R_j ($j < k$) has not broadcast the class of his action yet. Then R_j will take no advantage from the cheating. But he will not be caught either. This is because he can perform a collective measurement on χ_{k-1} and ψ to make the qubit ϕ received by R_{k+1} collapse to $\hat{U}(\varphi_k)|\chi_{k-1}\rangle$, where the class of the action corresponding to φ_k can be inferred from the result of his collective measurement. Later, when he is required to announce the exact value of φ_k for the valid runs in step (6), he can also infer this value since a run is recognized as valid only when all participants have announced their classes of actions so that $\left|\cos(\sum_j^N \varphi_j)\right|$ can be calculated in step (5). And φ_k can be calculated as long as R_k knows all the classes of actions of R_j ($j < k$). Thus he can always broadcast correctly.

(ii) All R_j ($j < k$) have broadcast the class of their action. Then it is sufficient for R_k to determine a proper basis so that he can know the exact state of χ_{k-1} by measuring it. He also measures ψ to collapse ϕ into either $|\pm x\rangle$ or $|\pm y\rangle$, and he compares the result of ϕ with the state of χ_{k-1} to infer the correct value of φ_k to broadcast. Again, his cheating will not be detected. But in this case he knows the exact state of χ_{k-1} and χ_k without the help of any other participants. Then a subset of less than $N-1$ participants with R_k included will be able to infer the choice of φ_R of another participant.

Responding to this cheating strategy, Schmid *et al.* proposed a modified protocol [9], where they attempt to ensure that the second case never occurs and thus would make the cheating futile.

Modified protocol 1:

All steps are the same as those of the original protocol, except that in step (4), the order in which the participants announce the classification is no longer random, but always reverse to the order of the qubit transmission. That is, since in step (2) the qubit is passed through the participants in the order $R_1 \to R_2 \to ... \to R_{N-1} \to R_N$, in step (4) the class choice must be revealed in the order $R_N \to R_{N-1} \to ... \to R_2 \to R_1$.

This modified protocol indeed evades the second case of the cheating strategy, however, it is still insecure with even poor security, as shown below.

Cheating strategy B:

Similar to cheating strategy A, after the dishonest participant R_k ($k \in \{2, ..., N-1\}$) receives the qubit χ_{k-1} from R_{k-1}, he does not apply $\hat{U}_k(\varphi_k)$ on it and pass it to R_{k+1}. He prepares an EPR pair $|\psi\phi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, and sends the second qubit ϕ to R_{k+1} as χ_k while keeping ψ to himself. But the difference is that he needs not to keep χ_{k-1} unmeasured in this strategy. Instead, he can measures it immediately in the basis $|\pm x\rangle$ or $|\pm y\rangle$.

In step (4), when it is time for R_k to broadcast the class of his action, all R_j ($j > k$) have broadcast the class of their action since it was suggested in modified protocol 1 that the class choice is broadcast in the reversed order. R_k then counts the number of the class Y action among R_j ($j > k$). If the number is even (or odd), he measures the qubit ψ in the basis $|\pm x\rangle$ (or $|\pm y\rangle$). Thus he can infer the state of ϕ (i.e., χ_k) from the entangled form of $|\psi\phi\rangle$. By comparing the state with the result in his previous measurement on χ_{k-1}, he can always infer the exact value of φ_k and finish the rest of the protocol successfully, just as if he had applied the operator $\hat{U}_k(\varphi_k)$ on χ_{k-1} and then passed it to R_{k+1} without cheating. But unlike the honest protocol, in this case he always knows the exact states of both χ_{k-1} and χ_k for any valid run. Therefore among the first k participants (i.e., all R_j with $j \leqslant k$), any subset of $N' = k-1$ participants with R_k included can infer the choice of φ_R of the remaining participant. Also, among the last $N-k+1$ participants (i.e., all R_j with $j \geqslant k$), any subset of $N' = N-k$ participants with R_k included can infer the choice of φ_R of the remaining participant. Especially, if the participant R_2 (R_{N-1}) cheats with this strategy, he alone can always know the choice of φ_1 (φ_N) of the first (last) participant.

Therefore, the modified protocol 1 is not secure either. Moreover, unlike the case of the original protocol, where the cheating strategy A can only gain information on the secret data in certain cases, the cheating strategy B can always be successful for the modified one. In addition, the cheating strategy B is more feasible to be implemented, because no collective measurements on χ_{k-1} and ψ are required, while they are needed in the cheating strategy A. The cheater here even needs not to store the

qubit χ_{k-1} for a long period of time. Consequently, the modified protocol 1 proposed in Ref.[9] is even less secure than the original one.

If we want to defeat only the above cheating strategies alone, we would have the following simple solution.

Modified Protocol 2:

All steps are the same as those of the original protocol, except that in step (4), the order in which the participants announce the classification can be arbitrary, as long as the participants R_1 and R_N are always the last two to announce.

With this modification, when R_k ($k \in \{2, ..., N-2\}$) broadcasts the class of his action in step (4), the cases where either all R_j ($j > k$) or all R_j ($j < k$) have broadcast the classes of their actions will never occur. Meanwhile, R_1 and R_N can gain no extra information from this modification, because the state of the qubit they send or receive are always known to them even in the honest protocol. Thus the protocol is made secure against the above two cheating strategies.

Unfortunately, there are still some serious drawbacks in this one. First, it cannot stand the multi-cheater attack. Suppose that there are two cheaters, R_k ($k \in \{2, ..., N-2\}$) and R_1 (or R_N), and they exchange information secretly. Then although R_1 and R_N are always the last two to announce the classes of actions, it is still possible for R_k to know the classes of actions of all R_j ($j > k$) or all R_j ($j < k$) before he announces his own. This is because R_N (or R_1) may tell R_k his choice secretly, or they may even have agreement beforehand on the routine on how R_N (or R_1) makes his choice so that they need not to communicate during the process of the protocol. Thus one of the above cheating strategies may still work. Similarly, even if we put further restrictions on the order of the broadcast of the classes of actions (e.g., by fixing the order as $R_{N/2} \to R_{N/2+1} \to R_{N/2-1} \to R_{N/2+2} \to ... \to R_1 \to R_N$ when N is even), it is still possible to cheat if more participants are dishonest. Second, none of the above three versions is able to locate the cheater(s). Even if the participants find disagreed announcement in the security check, what they know is merely the existence of cheater(s), but they never know exactly who is(are) cheating. Because of this, a dishonest participant surely inclines to cheat as he is benefitted from a successful cheating while has no risk to be caught, even if the cheating fails. In fact, even if a cheater does not have the technical power to implement the above cheating strategies, he can still cheat with the simple intercept-and-resend attack. That is, when he receives the qubit, he simply measures it with a randomly chosen basis and then passes it to the next participant. Indeed, as shown in Ref.[7], this cheating stands a non-trivial probability to be detected. But since the participants cannot locate which one is the cheater and the information obtained by the cheater is also non-trivial when the cheating is successful, a dishonest participant surely likes to take the risk.

To achieve a mission of unconditional security, below we present a secure protocol with a distinct security checking strategy.

Our secure protocol:

(I) The N participants agree on the number n of the total runs of the qubit communication, a weight w ($w > 0.6n$ is recommended), and a Boolean matrix G as the generating matrix of a binary linear (n, k, d)-code C [10], where d satisfies $n[1 - 4w^2/(3n^2 - 2nw + 3w^2)] < d < 2(n - w)$. Each participant R_j ($j = 2, ..., N-1$) chooses secretly an n-bit codeword $c_j = (c_{j1}c_{j2}...c_{jn})$ from C whose weight (the number of 1 in c_j) is w.

(II) For $i = 1$ to n:

(II-1) The first participant R_1 prepares a single qubit in the state $|+x\rangle$.

(II-2) The qubit is passed through the N participants sequently. Each participant R_j ($j = 1, ..., N$) applies an action on the qubit. For the participant R_j ($j = 2, ..., N-1$), the action is chosen according to the ith bit of the codeword c_j. If $c_{ji} = 0$, R_j applies a class X or Y action; else if $c_{ji} = 1$, R_j applies a class Z action. The participants R_1 and R_N apply the class X or Y action only. Here, the class X and Y actions are defined as the same as those in the original protocol. The class Z action means that R_j chooses the secret data $\varphi_{j1} \in \{0, \pi/2\}$ and acts on the qubit with $\hat{U}_j(\varphi_{j1})$, then measures the qubit in the basis $|\pm x\rangle$. He then chooses another secret data $\varphi_{j2} \in \{0, \pi/2, \pi, 3\pi/2\}$ and acts on the measured qubit with $\hat{U}_j(\varphi_{j2})$, and sends the qubit to the next participant. All these φ are independently chosen for each run.

(II-3) The last participant R_N measures the qubit in the basis $|\pm x\rangle$.

(III) For $i = 1$ to n, each participant R_j ($j = 2, ..., N-1$) announces the bit c_{ji} in random order.

(IV) Security check 1: the participants check whether each c_j ($j = 2, ..., N-1$) is a codeword from C with the weight w.

(V) For $i = 1$ to n, the participants who announced $c_{ji} = 0$ broadcast the classes of their actions in random order.

(VI) The participants determine which runs are valid runs, i.e., the runs which contain no class Z action (i.e., $c_{ji} = 0$ for $\forall j \in \{2, ..., N-1\}$) and satisfy $\left|\cos(\sum_j^N \varphi_j)\right| = 1$.

(VII) Security check 2: the participants choose a subset of valid runs and all the runs containing the class Z action. For each valid run, each participant announces his choice of φ_j in random order. They compare these values with the measurement result in step (II-3) to detect cheating. For each run containing the class Z action, the participants who applied the class X or Y action (except R_1 and R_N) announce their choices of φ_j in random order. Then R_1, R_N and these who applied the class Z action announce all their choices of φ_{j1} (including φ_N) and the results of the measurement first and then φ_{j2} (including φ_1), and check whether they are in agreement with the announcements of the other participants.

(VIII) When no disagreement is found, the task of secret sharing is thus achieved with any of the remaining valid runs. When any subset of $N-1$ participants want to infer the choice of φ_R of the remaining participant, they reveal among themselves their values of φ_j and the measurement result in step (II-3) if the last participant is included in this subset.

Obviously this protocol can accomplish the task that any subset of $N-1$ participants can infer the choice of φ_R of the remaining participant if they collaborate. Also, the protocol can meet the requirement that any subset of less than $N-1$ participants cannot infer the choice of φ_R of a honest participant, as shown below.

Let us consider the most severe case where $N-2$ participants are cheaters, and they can exchange any information they know. Surely, if the protocol is proven to be secure in such a setting, it is secure in any other settings. In the following it will be rigorously proven that the $N-2$ cheaters cannot infer the secret choice of each of the two honest participants without being detected, unless with a probability which can be made arbitrarily small as n increases.

Let R_a and R_b $(a<b)$ denote the two honest participants. Consider first the case where R_a and R_b are neighbors in the qubit transmission, i.e., $b=a+1$. Obviously the other $N-2$ cheaters can infer the value of $\cos(\varphi_a+\varphi_b)$ only, instead of each secret data φ_a or φ_b alone, unless they perform a man-in-the-middle eavesdropping attack between R_a and R_b. But similar to the well-accepted security of the BB84 quantum key distribution protocol[11], it is easy to understand that the eavesdropper cannot escape from being detected when R_a and R_b both apply the class Z action. Therefore, to infer any one of φ_a or φ_b, the $N-2$ cheaters still need to collaborate with either R_b or R_a, i.e., the collaboration of $N-1$ participants is needed so the protocol is secure.

Secondly, consider the case where R_a and R_b are separated. Since the object of the cheaters is to learn the state of the qubit sent by R_a (or received by R_b) so that φ_a (or φ_b) can be inferred, at least one cheater R_k $(a<k<b)$ between R_a and R_b must replace the honest action with a cheating one. In this cheating action, R_k must stop the qubit sent by R_a so that its state can be learned, and he sends the next participant another qubit to continue with the protocol. The above cheating strategies A and B are both such examples. To pass the security checks, the cheating action must be able to be announced as a class X, Y or Z action when needed. But this cannot always be done, as proven by the following four steps.

(a) *To cheat successfully, the cheater R_k should be able to announce the cheating action as a class X or Y action.* An honest class X or Y action cannot be announced as a class Z action, because the participant cannot announce the result of the measurement on the qubit he received correctly since he did not keep it. Therefore, although a cheating action can always be announced as a class Z action, if it cannot be announced as a class X or Y action, R_k must apply the honest class X or Y action for exactly $n-w$ runs to pass security check 1. Then for any valid run, the action of R_k is honest, cheating being impossible.

(b) *R_k cannot announce the cheating action as a class X or Y action in a run where both R_a and R_b applied the class Z action, or he will be detected in security check 2 with a non-trivial probability.* To announce the cheating action as a class X or Y action correctly, R_k needs to know φ_k exactly. Similar to cheating strategies A and B, it can be seen that φ_k can be inferred if R_k knows the class choices of all R_j $(a\leqslant j<k)$ or all R_j $(k<j\leqslant b)$. But if both R_a and R_b applied the class Z action, they never need to announce their choice before R_k announces φ_k in security check 2. Thus R_k has to announce the value of φ_k by guess, and stands a non-trivial probability to be detected.

(c) *The number of runs in which R_k can announce the cheating action as a class X or Y action without being detected is not sufficient for R_k to pass security check 1.*

From point (b), it is seen that R_k can safely announce the cheating action as any of the class X, Y or Z action freely only in the runs where he is sure that either R_a or R_b applied a class X or Y action. Now let us evaluate the number of these runs.

In each of the first $n-d$ runs, R_k cannot know the choices of c_{ji} of R_a and R_b before they announce, because the number of possible codewords is at the order of magnitude of 2^k when $d<2(n-w)$. Since in step (III) c_{ji} is announced in a random order, there are three possibilities: both R_a and R_b announced before R_k does; one and only one of R_a and R_b announced before R_k does; none of R_a and R_b announced before R_k does. The probabilities for these cases to occur are 1/4, 1/2, and 1/4, respectively. In the first two cases R_k can be sure of the class of action of R_a and/or R_b. Since each participant should apply the class Z action w times, the probability for $c_{ai}=0$ (or $c_{bi}=0$) is $1-w/n$. Therefore, the probability for such a run to be the one in which R_k can announce the cheating action as a class X or Y action is

$$p_1=(1-w^2/n^2)/4+(1-w/n)/2. \tag{2}$$

In each of the last d runs, since the string c_j of each participant R_j must be a codeword of C and the minimum distance between codewords is d, the choice of c_{ji} $(i\in\{n-d+1,..,n\})$ of each participant can be inferred by the others from the announced c_{ji} $(i\in\{1,..,n-d\})$ of the first $n-d$ runs. Thus R_k knows the choice of action of R_a and R_b before they announce. The probability for such a run to be the one in which R_k can announce the cheating action as a class X or Y action is then

$$p_2=1-w^2/n^2. \tag{3}$$

Totally, even if R_k applies the cheating action in all the n runs, the maximum number of runs in which he can

announce the cheating action as a class X or Y action is

$$\begin{aligned} n' &= (n-d)p_1 + dp_2 \\ &= (n-d)[(1-w^2/n^2)/4 + (1-w/n)/2] \\ &\quad +d(1-w^2/n^2). \end{aligned} \tag{4}$$

Therefore, after R_k finishes applying all the actions (either honest or cheating ones) on the n qubits in step (II), the major part of the n-bit string c_k which he can announce in step (III) is already determined. Only n' bits at the most can be altered between 0 and 1 by R_k according to the announcement of R_a and R_b, while the other bits have to be announced honestly or announced as 1. Since it is suggested in the protocol to choose $d > n[1-4w^2/(3n^2-2nw+3w^2)]$, from the above equations it can be verified that $d > n'$. According to the property of the binary linear (n,k,d)-code C [10], altering less than d bits of a codeword will not result in another codeword since the distance between any codewords is not less than d, except with a trivial probability. Therefore, among all the possible strings which can be obtained by altering no more than n' bits of c_k, only those less than $1/\binom{n-n'/2}{n'/2}$ portion are valid codewords from C. Note that, which string is the one that can finally be announced by R_k is determined by the position of the runs in which R_a or R_b announced either $c_{ai}=0$ or $c_{bi}=0$ before R_k announces c_{ki}. Due to the random order of the announcement, R_k will generally not be so lucky that the final string which he can announce happens to be a valid codeword while has also the weight w exactly, except with a probability which can be made arbitrarily small by increasing n. Thus R_k cannot pass security check 1 by altering n' bits of c_k.

(d) *Seen from the above points, the probability for R_k to cheat successfully is arbitrarily small as n increases.* Point (c) ensures that R_k is unable to cheat successfully by altering his announcement on the choice of action only in the runs in which R_a or R_b announced either $c_{ai}=0$ or $c_{bi}=0$ before R_k announces c_{ki}. On the other hand, a dishonest R_k may take the risk to announce the cheating action as a class X or Y action in the runs where both R_a and R_b applied the class Z action, so that the announced string c_k can be a valid codeword with the weight w. But it was proven in point (b) that in any single run, announcing the cheating action as a class X or Y action stands a non-trivial probability to be detected. Let ε denotes this probability. Since the minimum distance d between codewords increases with n, the number of runs in which both R_a and R_b applied the class Z action while R_k needs to announce the cheating action as a class X or Y action to make c_k valid will also grow as n increases. Thus the total probability for R_k to pass the whole protocol without being detected will be $(1-\varepsilon)^{O(n)}$, which can be made arbitrarily small by increasing n.

At this stage, it is seen that no cheating could be successful with a non-trivial probability. Moreover, when R_a and R_b detected cheating, they know that the cheater is located between a and b. In the case where $b=a+2$ or more participants are honest and n is sufficiently large so that the values of a and b run through many different combinations, the cheater can be more precisely located.

We wish to emphasize that, implementation of our protocol involves merely single qubit operations, which may easily be realized with the technology reported in Ref.[7]. For example, by pumping a β-barium borate (BBO) crystal with a violet single mode laser diode, photons can be generated via a type II spontaneous parametric down conversion (SPDC) process. The initial polarization state can be prepared by placing a polarizer vertically in front of a trigger detector ensuring that only horizontally polarized photons are used. The first participant uses a half-wave plate followed by a quarter-wave plate at an angle of 45°. By rotating the half-wave plate to the angles 0°, 45° and 22.5°, −22.5° he could apply the phase shifts $\varphi_1 \in \{\pi/2, 3\pi/2\}$ and $\varphi_1 \in \{0,\pi\}$ on the horizontally polarized photons to transform them into $|\pm y\rangle$ and $|\pm x\rangle$. As the photon passes through the participants, each of them can apply the phase shift φ_j using yttrium vanadate (YVO_4) crystals, which were cut such that their optic axis lies parallel to the surface and is aligned in such a way that horizontal and vertical polarization states correspond to their normal modes. By rotating the crystals along the optic axis for a certain angle, a specific relative phase shift φ_j can be applied independently from the incoming polarization state. Measurement of the photons can be done by detecting them with passively quenched silicon avalanche photo diodes (Si-APD) behind a half-wave plate at an angle of 22.5° followed by a polarizing beam splitter. The rest part of the class Z action, i.e., applying another phase shift φ_{j2} on the measured photon and then resending it to the next participant, can be done by preparing another independent photon from the photon source and then adjusting its polarization to the proper value with half-wave and quarter-wave plates, with devices like those of the first participant.

The work was supported by the NSFC under grant Nos.10605041 and 10429401, the NSF of Guangdong province under grant No.06023145, and the Foundation of Zhongshan University Advanced Research Center.

[1] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
[2] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[3] R. Cleve, D. Gottesman, and H. -K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[4] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).
[5] Y. -A. Chen, A. -N. Zhang, Z. Zhao, X. -Q. Zhou, C. -Y.

Lu, C. -Z. Peng, T. Yang, and J. -W. Pan, Phys. Rev. Lett. **95**, 200502 (2005).
[6] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, Phys. Rev. Lett. **98**, 020503 (2007).
[7] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Phys. Rev. Lett. **95**, 230505 (2005).
[8] G. P. He, Phys. Rev. Lett. **98**, 028901 (2007).
[9] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Phys. Rev. Lett. **98**, 028902 (2007).
[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1977).
[11] C. H. Bennett, and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, 1984 (IEEE, New York, 1984), p.175.